Claims

1. A method of exchanging digital data between a first party having a unique first digital data and a second party having a unique second digital data over a communication link, the method comprising the steps of:

(a) the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party;

(b) the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party if the verification is positive;

(c) the first party verifying that the second digital data is valid, and if the verification is positive the first party accepts the second digital data and sends the unencrypted first digital data to the second party;

(d) the second party verifying that the first digital data is valid, and if the verification is positive, the second party accepts the first digital data; otherwise, the second party sends the encrypted first digital data and the second digital data to a third party, third party having a decryption key to decrypt the encrypted first digital data; and

(e) the third party decrypting the encrypted first digital data to obtain the first digital data, verifying that the first and the second digital data are valid and, if both the first and the second digital data are verified as valid, sending the first digital data to the second party and the second digital data to the first party.

2. A method according to claim 1, in which the first and second digital data are on files M_A and M_B respectively, the first party in step (a) encrypting the first digital data on a concatenation of file M_A and a one-way hash of file M_B; and the second party in step(b), if the verification is positive, encrypting the second digital data on a concatenation of file M_B and a one-way hash of file M_A.

a

3. A method according to claim 1 ~~or claim 2~~, wherein the first and second digital data are digital signatures belonging to the first and second party, respectively.

4. A method according to claim 1, wherein the second digital data is a secret file M which the first party wishes to receive from the second party in exchange for the first digital data.

a

5. A method according to claim 1 ~~any of the preceding claims,~~ wherein

the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme.

6. A method according to claim 5, wherein the digital signature schemes are discrete logarithm based schemes; and the public key encryption scheme is a discrete logarithm based scheme.

7. A method according to claim 5, wherein the digital signature schemes are Guillou-Quisquater type digital signature schemes; and the public key encryption scheme is a discrete logarithm based scheme.